Recto

Retour sur les A-modules libres.

$M \qquad (e_i)_{i\in I}, \quad e_i \in M$

tq tout $x \in M$ s'écrive de manière unique $\sum_{i\in I} a_i e_i, \qquad a_i \in A$

$\{i \in I, \ a_i \neq 0\}$ fini

unicité $\Leftrightarrow$ $\{e_i\}_{i\in I}$ linéairement indépendants

Exemple. $\mathbb{Q}$ n'est pas un $\mathbb{Z}$-module libre.

$\{e_i ; i \in I\}$ libre $\Rightarrow |I| \leq 1$ qu $\frac{p}{q} - \frac{u}{v}$ $vp = 0$

Rang d'un A-module M : $rg_{\mathbb{Z}} M$ = nombre maximal d'éléments de M linéairement ind./A

Sous-A-module de torsion d'un A-module M

$$x \in M_{tors} \iff \exists a \in A, \ a \neq 0, \ ax = 0.$$

M est sans torsion si $M_{tors} = (0)$

M est de torsion si $M_{tors} = M$.

Théorème de structure des groupes abéliens G de type fini. G_{tors} est fini et

$G \simeq G_{tors} \times \mathbb{Z}^r \qquad r = \mathrm{rang}_{\mathbb{Z}} G$.

Cor. G groupe abélien libre de type fini $\iff G \simeq \mathbb{Z}^r$. | groupe fini $\iff r = 0$.

Exemple de groupe abélien de torsion infini (pas de type fini)

$$\underset{\text{additif}}{\mathbb{Q}/\mathbb{Z}} \simeq \underset{\text{mult.}}{U}$$

$$U = \mathbb{C}^\times_{tors} = \{\zeta \in \mathbb{C}, \ \exists n \geq 1, \ \zeta^n = 1\}$$

racines de l'unité

$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C}^\times \\ \rotatebox{90}{$\in$} & & \\ z & \longmapsto & e^{2i\pi z} \end{array}$$

$$\begin{array}{ccc} \mathbb{C}/\mathbb{Z} & \xrightarrow{\sim} & \mathbb{C}^\times \\ \cup & & \cup \\ \mathbb{R}/\mathbb{Z} & \xrightarrow{\sim} & \{z \in \mathbb{C}, \ |z| = 1\} \\ \cup & & \cup \\ \mathbb{Q}/\mathbb{Z} & \longrightarrow & U \end{array}$$

Discriminant.

$A \subset B$ anneaux

B est un A-module libre de type fini.

$n = \mathrm{rang}_A B$.

$$\begin{array}{cccc} D_{B/A} : & B^n & \longrightarrow & A \\ & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ & (x_1, \dots, x_n) & \longmapsto & \det\left(Tr_{B/A}(x_i x_j)\right)_{1\leq i,j\leq n} = D_{B/A}(x_1, \dots, x_n) \end{array}$$

Exemple

$A = K$ corps $\quad d \in K$ pas un carré

$X^2 - d \qquad B = K(\sqrt{d})$ corps

$n = 2$

$x_1 = 1$

$x_2 = \sqrt{d}$.

$$D_{B/A}(1,\sqrt{d}) = \det \begin{pmatrix} Tr_{B/A} 1 & Tr_{B/A} \sqrt{d} \\ Tr_{B/A} \sqrt{d} & Tr_{B/A} d \end{pmatrix}$$

$$= \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

$B = K(\sqrt{d})$
$\cup$
$A = K \quad \ni 1, d.$

$Tr_{B/A}(a) = 2a$

$a \in A$

$[a] : B \longrightarrow B$
$y \longmapsto ay$

$a \in A$

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

$[\sqrt{d}] : K[\sqrt{d}] \longrightarrow K[\sqrt{d}]$

base $1, \sqrt{d}$.

$$\begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix}$$

$Tr_{B/A}(\sqrt{d}) = 0$

Remarque ($A = K$) Si Car $K = 2$, $D_{B/A} = 0$

Exemple en caractéristique 2.

$K = \mathbb{F}_2(T) \qquad X^2 - T \in K[X]$ irréductible.

$K(\sqrt{T}) \ni x_1, x_2 \qquad D_{K(\sqrt{T})/K}(x_1, x_2) = 0$

$\mid 2$

K

Extension non séparable.

Lemme. $A \subset B$, B A-module libre de type fini de rang n. Soient $M = (a_{ij})_{1 \le i,j \le n}$ et $(x_1, \dots, x_n) \in B^n$.

$\cap$

$Mat_{n \times n}(A)$

On pose $\displaystyle y_i = \sum_{j=1}^{n} a_{ij} x_j \qquad 1 \le i \le n.$

Alors $D_{B/A}(y_1, \dots, y_n) = (\det M)^2 \cdot D_{B/A}(x_1, \dots, x_n)$

Dém. $Tr_{B/A} : B \to A$ bilinéaire.

Si M est inversible dans $Mat_{n \times n}(A)$

alors $\det M \in A^\times$

$(\det M)^2 \in A^\times$

et $D_{B/A}(x_1, \dots, x_n)$ et $D_{B/A}(y_1, \dots, y_n)$ engendrent le même idéal de A.

Déf. Idéal discriminant de B sur A

$\mathfrak{D}_{B/A}$ = idéal principal de A engendré par $D_{B/A}(x_1, \dots, x_n)$ pour une base $(x_1, \dots, x_n)$ de B sur A

Indépendant du choix de la base.

Cas particulier $A = \mathbb{Z}$.

B anneau $\mathbb{Z}$-module libre de type fini.

$n = \mathrm{rang}_{\mathbb{Z}} B$ $\quad e_1, -, e_n$ une base

$D_{B/\mathbb{Z}}(e_1, -, e_n)$ est indépendant du choix de la base.

$\| \quad D_B$ discriminant absolu de B $\in \mathbb{Z}$.

Lemme. Supp. $\mathfrak{D}_{B/A} \neq (0)$

Soit $(x_1, -, x_n) \in B^n$.

Alors $x_1, -, x_n$ est une base de B comme A-module $\Longleftrightarrow D_{B/A}(x_1, -, x_n)$ engendre $\mathfrak{D}_{B/A}$.

Démonstration

$\Rightarrow$ c'est la définition de $\mathfrak{D}_{B/A}$.

$\Leftarrow$ $e_1, -, e_n$ une base de B/A.

$x_i = \sum_{j=1}^{n} a_{ij} e_j \qquad M = (a_{ij})$

$e_1, -, e_n$ base $\quad D_{B/A}(e_1, -, e_n)$ engendre $\mathfrak{D}_{B/A}$

$(x_1, -, x_n) \in B^n \quad D_{B/A}(x_1, -, x_n)$ engendre $\mathfrak{D}_{B/A}$ idéal de A

$D_{B/A}(x_1, -, x_n) = u\, D_{B/A}(e_1, -, e_n) \quad u \in A^\times$.

$D_{B/A}(x_1, -, x_n) = (\det M)^2 \cdot D_{B/A}(e_1, -, e_n)$

$\left((\det M)^2 - u\right) \cdot \underbrace{D_{B/A}(e_1, -, e_n)}_{\neq 0} = 0 \qquad A$ intègre.

$(\det M)^2 = u. \qquad \mathfrak{D}_{B/A} = (0)$

$\Rightarrow \det M \in A^\times \Rightarrow M$ inversible $\Rightarrow x_1, -, x_n$ base B/A

$A = \mathbb{Z}$ $\quad$ discriminant $(x_1, -, x_n)$ $\neq \pm 1$ $\quad \neq 0$

$\cap$

B

le sous-$\mathbb{Z}$-module engendré par $x_1, -, x_n$ est d'indice fini dans B et $\neq B$.

Proposition. $L|K$ extension finie séparable $n = [L:K]$. N extension de L, $N|K$ normale

$\sigma_1, -, \sigma_n$ les K-homomorphismes de L dans N.

$x_1, -, x_n \in L$ $\quad \boxed{D_{L/K}(x_1, -, x_n) = \left(\det\left(\sigma_k x_i\right)_{1 \le i, k \le n}\right)^2}$

Démonstration.

$$Tr_{L|K}(x_i x_j) = \sum_{h=1}^{m} \sigma_h(x_i)\sigma_h(x_j)$$

det

$D_{L|K}(x_1, \dots, x_n)$ $\qquad (\det(\sigma_h x_i))^2$.

Cas particulier : $L = K(\alpha)$ $\qquad n = [L:K]$.

$\{x_1, \dots, x_n\} = \{1, \alpha, \dots, \alpha^{n-1}\}$

$\alpha_1, \dots, \alpha_n$ les conjugués de α dans N

$N \,|\, K(\alpha) \,|\, K$

$$Tr_K(\alpha; X) = \prod_{i=1}^{n}(X - \alpha_i)$$

$$D_{L|K}(1, \alpha, \dots, \alpha^{n-1}) = \left(\det\left(\alpha_h^{i-1}\right)_{1 \le h, i \le n}\right)^2$$

$$= (-1)^{\frac{n(n-1)}{2}} \prod_{1 \le i \ne j \le n} (\alpha_i - \alpha_j) = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)^2$$

Définition. A anneau. $P(X) = a_0 X^n + \dots + a_n$.

K corps des fractions $\qquad \deg P = n$

N corps de décomposition de P sur K. $\qquad a_0 \ne 0$.

$\alpha_1, \dots, \alpha_n$ racines de P dans N. $\quad P(X) = a_0 \prod_{i=1}^{n}(X - \alpha_i)$

$$D(P) = a_0^{n(n-1)} (-1)^{\frac{n(n-1)}{2}} \prod_{1 \le i \ne j \le n} (\alpha_i - \alpha_j).$$

Exercice.

$A = \mathbb{Z}$. $\qquad P \in \mathbb{Z}[X]$

signe de $D(P)$ disc. de P $\qquad$ degré n. $\quad a_0 > 0$.

$(-1)^{r_2}$.

n racines distinctes dans $\mathbb{C}$.

$$P(X) = a_0 \cdot \underbrace{f_1 \cdots f_{r_1}}_{\deg 1}, \underbrace{f_{r_1+1} \cdots f_{r_1+r_2}}_{\deg 2.} \qquad n = r_1 + 2r_2$$

décomposition de P en facteurs irréductibles dans $\mathbb{R}[X]$.

f_i unitaires.

$X - \alpha \qquad \alpha \in \mathbb{R}$

$X^2 + bX + c = (X - \alpha)(X - \bar{\alpha}) \qquad b^2 - 4c < 0$

$\alpha \in \mathbb{C} \setminus \mathbb{R}$.

P a r_1 racines réelles

$2r_2$ racines non réelles. (complexes conjuguées)

$\mathbb{Q}(\alpha) \,|_n\, \mathbb{Q}$ $\qquad P(\alpha) = 0 \qquad P(X) = \prod_{i=1}^{n}(X - \alpha_i)$

$n = \deg P$.

il y a n homomorphismes

$$\varphi : \mathbb{Q}(\alpha) \longrightarrow \mathbb{C}, \quad \alpha \longmapsto \alpha_i$$

r_1 est le nombre d'homomorphisme de $\mathbb{Q}(\alpha)$ dans $\mathbb{R}$. $\qquad \tau \circ \varphi = \varphi$

$2r_2$ est le nombre d'homomorphismes de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$ dont l'image n'est pas réelle. $\qquad \tau \circ \varphi \ne \varphi$

$$\tau : \mathbb{C} \longrightarrow \mathbb{C}, \quad z \longmapsto \bar{z}$$

Entiers algébriques

$\mathbb{Q} \subset k$ $\qquad$ k corps de nombres.

$\cup$

$\mathbb{Z}$ $\qquad$ $\mathbb{Z}_k$ anneau des entiers de k

Lemme. A anneau (intègre), K corps $\ni A$

$\alpha \in K$. Propriétés équivalentes.

(i) α est racine d'un polynôme unitaire coeff $\in A$

(ii) $A[\alpha]$ est un A-module de type fini.

(iii) $\exists B$ sous-anneau de K, $A \subset B$, $\alpha \in B$,

B A-module type fini.

Déf. α est entier sur A.

Exemples. $A = \mathbb{Z}$ $\quad K = \mathbb{Q}$. $\qquad \alpha \in \mathbb{Q}$.

(i) $X - a \in \mathbb{Z}[X]$ $\qquad a \in \mathbb{Z}$

unitaire

racine α. $\qquad \alpha \in \mathbb{Z}$.

(ii) $\mathbb{Z}[\alpha] = \left\{ a_0 + a_1\alpha + \dots + a_n\alpha^n, \; n \geq 0 \quad a_i \in \mathbb{Z} \right\}$

t.g. comme $\mathbb{Z}$-module.

$\alpha = \frac{p}{q}$. $\qquad 1, \alpha, \dots, \alpha^{m-1}$. syst gén. $/\mathbb{Z}$

$\alpha^m = \left(\frac{p}{q}\right)^m \quad \Rightarrow q = \pm 1 \quad \alpha \in \mathbb{Z}$

$\mathbb{Z}[\alpha]$ $\quad$ $\mathbb{Z}$-module t.g.

$\exists \beta_1, -, \beta_\ell \in \mathbb{Z}[\alpha]$ t.q.

tout elt de $\mathbb{Z}[\alpha]$ soit comb. lin.

de $\beta_1, -, \beta_\ell$ coeff dans $\mathbb{Z}$.

$m-1 =$ + grand degré des polynômes en α

exprimant $\beta_j \in \mathbb{Z}[\alpha]$

Tout elt de $\mathbb{Z}[\alpha]$ est comb. lin. de $1, \alpha, -, \alpha^{m-1}$.

$\alpha^m = c_0 + c_1\alpha + - + c_{m-1}\alpha^{m-1}$. $\qquad \alpha = \frac{p}{q}$.

$p^m = c_0 q^m + c_1 p q^{m-1} + \dots + c_{m-1} p^{m-1} q \qquad$ pgcd$(p,q) = 1$

$\Rightarrow q = \pm 1$.

Démonstration.

(ii) $\Rightarrow$ (iii) $\qquad$ (ii) $A[\alpha]$ est un sous-anneau contenant A et α qui est un A-module de t.g.

(i) $\Rightarrow$ (ii) $\qquad X^m + a_1 X^{m-1} + \dots + a_m \in A[X]$

montrons. $\boxed{\alpha^m = -a_m - a_{m-1}\alpha - \dots - a_1\alpha^{m-1}}$.

$A[\alpha] \supseteq \underbrace{A + A\alpha + \dots + A\alpha^{m-1}}_{\text{est un anneau}}$ ..

trivial

But

$\alpha^\ell \in A + A\alpha + - + A\alpha^{m-1}$ $\qquad$ vrai pour $\ell = 0, 1, .., m-1$

$\forall \ell \geq 0$ $\qquad$ et $\ell = m$.

Supp. $\alpha^{\ell} \in A + A\alpha + \dots + \underline{A\alpha^{m-1}}$.

$\alpha^{\ell+1}$

$$A\alpha^{m} \subset A + A\alpha + \dots + A\alpha^{m-1}.$$

(iii) $\Rightarrow$ (i) La prochaine fois